723931_1
Docket No · 3423 1004-001
MLW/WH/

PROPOSED CLAIM AMENDMENT (AFTER ALLOWANCE)

Claim Listing:

1. (Previously presented) A method implemented in a processor system for a sender to encrypt an electronic message prior to sending to a receiver, comprising the steps of:

   generating an ad hoc public key and private key asymmetric key pair that is uniquely associated with both the sender and the receiver;

   encrypting the private key, the private key known only to the sender;

   creating an index value that is uniquely associated with the key pair and both the sender and the receiver, the index value utilized for key retrieval;

   storing in a key server at least the encrypted private key together with the associated index value; and

   encrypting the electronic message by utilizing the public key.

2. (Canceled)

3. (Previously presented)The method of claim 1 wherein the index value is known only to the sender.

4. (Previously presented) The method of claim 3 wherein the creating step comprises the steps of:

   obtaining an identity value by utilizing at least a unique identification for the sender and a unique identification for the receiver; and

   computing from the identity value an index value by utilizing a sender secret, the index value uniquely associated with the key pair, the index value utilized for key retrieval and known only to the sender.

5. (Canceled)

6. (Previously presented) The method of claim 1 wherein the key pair is a set of at least one key pair, each key pair associated with a validity field.

7. (Previously presented) The method of claim 1 wherein the ad hoc public key and private key asymmetric key pair is an ad hoc symmetric key.

8. (Previously presented) A method implemented in a processor system for a receiver to decrypt an encrypted electronic message received from a sender, comprising the steps of:

authenticating the receiver to the sender;

deriving an index value that is uniquely associated with an ad hoc public key and private key asymmetric key pair, the key pair uniquely associated with both the sender and the receiver;

retrieving an encrypted private key from a key server by utilizing the index value, the private key known only to the sender; and

decrypting the encrypted electronic message by utilizing the encrypted private key.

9. (Previously presented) The method of claim 8 wherein the decrypting step comprises the steps of:

obtaining an unencrypted private key from the encrypted private key by utilizing a sender secret; and

decrypting the encrypted electronic message by utilizing the unencrypted private key.

10. (Previously presented) The method of claim 8 wherein the index value is known only to the sender.

11. (Previously presented) The method of claim 10 wherein the deriving step comprises the steps of:

obtaining an identity value by utilizing at least a unique identification for the sender and a unique identification for the receiver; and

computing from the identity value an index value by utilizing a sender secret, the index value uniquely associated with an ad hoc public key and private key asymmetric key pair, the key pair uniquely associated with both the sender and the receiver, and the index value known only to the sender.

12. (Previously presented) The method of claim 8 wherein the electronic message is an electronic mail message.

13. (Previously presented) The method of claim 8 wherein the key pair is a set of at least one key pair, each key pair associated with a validity field, and the encrypted private key is selected from the set based on the validity field associated with the encrypted private key.

14. (Previously presented) The method of claim 8 wherein the ad hoc public key and private key asymmetric key pair is an ad hoc symmetric key.

15. (Previously presented) A processor system for a sender to encrypt an electronic message prior to sending to a receiver, comprising:

means for generating an ad hoc public key and private key asymmetric key pair that is uniquely associated with both the sender and the receiver;

means for encrypting the private key, the private key known only to the sender;

means for creating an index value that is uniquely associated with the key pair and both the sender and the receiver, the index value utilized for key retrieval;

means for storing in a key server at least the encrypted private key together with the associated index value; and

means for encrypting the electronic message by utilizing the public key.

16. (Previously presented) The system of claim 15 wherein the key pair is a set of at least one key pair, each key pair associated with a validity field.

17. (Previously presented) The system of claim 15 wherein the ad hoc public key and private key asymmetric key pair is an ad hoc symmetric key.

18. (Previously presented) A processor system for a receiver to decrypt an encrypted electronic message received from a sender, comprising:

means for authenticating the receiver to the sender;

means for deriving an index value that is uniquely associated with an ad hoc public key and private key asymmetric key pair, the key pair uniquely associated with both the sender and the receiver;

means for retrieving an encrypted private key from a key server by utilizing the index value, the private key known only to the sender; and

means for decrypting the encrypted electronic message by utilizing the encrypted private key.

19. (Previously presented) The system of claim 18, wherein the key pair is a set of at least one key pair, each key pair associated with a validity field, and the encrypted private key is selected from the set based on the validity field associated with the encrypted private key.

20. (Previously presented) The system of claim 18 wherein the ad hoc public key and private key asymmetric key pair is an ad hoc symmetric key.

21. (Previously presented) The method of claim 6 wherein encrypting the electronic message includes i) using a first key pair from the set of at least one key pair to encrypt a first electronic message, the first key pair associated with a valid first validity field; and ii) in an event the first validity field is not valid with respect to a second electronic message, using a second key pair from the set of at least one key pair to encrypt the second electronic message, the second key pair associated with a valid second validity field.

22. (Previously presented) The system of claim 16 wherein means for encrypting the electronic message includes i) means for using a first key pair from the set of at least one key pair to encrypt a first electronic message, the first key pair associated with a valid first validity field; and ii) in an event the first validity field is not valid with respect to a second electronic message, means for using a second key pair from the set of at least one key pair to encrypt the second electronic message, the second key pair associated with a valid second validity field.

23. (New) The method of claim 6 wherein the creating step includes creating an index value that is uniquely associated with the set of at least one key pair.

24. (New) The method of claim 13 wherein the deriving step includes deriving an index value that is uniquely associated with the set of at least one key pair.